SLAUGHTER AND MAY/

CLIENT BRIEFING

OCTOBER 2020

RELIEF FOR BRITISH AIRWAYS, BUT NOT FOR BUSINESSES FACING FINES IN THE FUTURE

On Friday 16th October, the Information Commissioner's Office (ICO) announced its long awaited fine of British Airways plc (BA) for breach of the General Data Protection Regulation (GDPR) following a cyber-attack in 2018. The final fine of £20 million, whilst being less than 1% of BA's turnover, is the second and largest fine issued by the ICO under the GDPR.

Background

As a quick reminder, the cyber-attack on BA started in its supply chain and led to the compromise of the sensitive financial data of over 400,000 customers and staff and was undetected for over two months.

The publication of the final fine follows extensive legal and technical submissions by BA since the original notice of intent in July 2019. The ICO had indicated in that an intention to fine BA £183.39 million, so the final penalty represents a significant reduction.

Whilst the ICO has found that BA failed to have appropriate security measures in place, BA has specifically not admitted the failings identified by the ICO.

So, what learnings can be taken from this?

The penalty notice details the ICO's views of BA's security failings, being both technical and organisational measures. This therefore provides a good checklist of the measures the ICO expects organisations to have in place.

The ICO specifically calls out a number of third party publications as either highlighting relevant vulnerabilities or which propose security measures. Given the importance that the ICO placed on these external publications, organisations should ensure that they have considered the publications the ICO refers to and any other relevant security guidance.

The notice also makes clear that prompt reporting to the relevant authorities and data subjects and taking steps to mitigate harms to data subjects (including offering to reimburse financial loss and free credit monitoring) played a significant part in the ICO's reduction of the fine. These findings once again emphasise the importance of organisations having well developed and tested response plans so that incidents are escalated with the right degree of urgency.

How was the fine calculated?

The most significant factor in the final fine being a lower amount than the earlier proposed fine appears to be the ICO's decision not to calculate the fine in line with its 'Draft Internal Procedure'. This is referred to as internal guidance that was prepared to assist the internal ICO team in implementing its published Regulatory Action Policy. This procedure included 'turnover bands as a starting point for the penalty calculation' which were not then applied in calculating the final BA fine.

Turnover was, however, still a relevant factor, with the ICO saying "it is self -evident that imposing the same penalty on an undertaking with a turnover of billions of pounds as would be imposed on a small or medium sized business would not be effective, proportionate or dissuasive."

The ICO ultimately determined that a £30 million fine would be appropriate and this was then reduced by 20%, to £24 million, to reflect mitigating factors. The fine was reduced by a further £4 million to reflect the impact of COVID-19.

What does this mean for future fines?

A public consultation on the Statutory guidance on the ICO's regulation policy was launched in October 2020. Contrary to the calculation of the final BA fine, the ICO's proposal provides that the starting point for all fines should be turnover-based, including a matrix to this effect.

The BA fine should not therefore be taken as indicative of the level of future fines for breaches of this seriousness. Instead, future fines will be calculated in line with the statutory guidance, once finalised and implemented, and could lead to the ICO imposing fines of the scale originally proposed against BA.

The ICO's final fine against Marriott following the data breach in its Starwood subsidiary is due to be published later this year, and so it will be interesting to see how the amount of that compares – it was originally proposed by the ICO to be £99 million.

It is also worth organisations remembering that the costs of a breach of the GDPR do not stop with regulatory enforcement action. Follow on litigation from data subjects could ultimately be more costly than the regulatory fine itself. The claim brought by data subjects against BA is working its way through the court process so the final cost to BA of the data breach will not be known for some time.

CONTACT

REBECCA COUSIN
PARTNER
T: +44(0) 20 7090 3049
E: rebecca.cousin@slaughterandmay.com

LUCIA BIRD
ASSOCIATE
T: +44(0) 20 7090 5365
E: lucia.bird@slaughterandmay.com